In the Specification:

The paragraph at page 1, lines 3-4, is amended as follows:

A1

The present invention relates to methods ~~and apparatus~~ for verifying the authenticity of partners in an electronic transaction.

The paragraph at page 2, line 17, is amended as follows:

A2

An alternative encryption scheme that provides enhanced security at relatively small modulus is that utilizing elliptic curves in the finite field 2^m. A value of m in the order of 155 provides security comparable to a 512 bit modulus for RSA and therefore offers significant benefits in implementation. Diffie Helman Public Key encryption utilizes the properties of discrete logs so that even if a generator β and the exponentiation β^k ~~is~~ are known, the value of k cannot be determined.

On page 3, after line 2, please insert the following subtitle:

A3

--SUMMARY OF THE INVENTION--

The paragraph at page 3, line 7, is amended as follows:

A4

The protocol disclosed is appropriate for smartcard purchase applications such as those that might be completed between a terminal or ATM and a user's ~~users~~ personal card. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is ~~an~~ a computationally intense operation for the smart card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol). In the preferred embodiment, the protocol ~~provides~~ protects the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.

The paragraphs beginning on page 3, lines 15 to 29, through page 4, lines 1 to 22, are deleted and replaced with the following new paragraph:

--In accordance with an embodiment of the invention, a method of performing a transaction between a first and a second participant is provided wherein the second participant permits a service to be provided to the first participant in exchange for a payment. The method comprises the steps of the first participant verifying the legitimacy of the second participant to obtain assurance that the service will be provided upon payment, the second participant verifying the legitimacy of the first participant to obtain assurance that payment will be secured upon provision of the service, and the second participant obtaining a digital signature for the first participant on the transaction whereby the second participant may obtain payment from a third participant.--

On page 4, after line 22, insert the following subtitle:

--BRIEF DESCRIPTION OF THE DRAWING--

On page 4, after line 27, insert the following subtitle:

--DESCRIPTION OF THE PREFERRED EMBODIMENTS--

The paragraph at page 5, line 22, is amended as follows:

The component rl is provided by $M2*Y_t^k$, mod L, ~~$M2.Y_t^k$ mod L~~ where:

M2 is the message TA//TIU ID//R2//PID, and

$L = 2^{\ell} - 1$ and ℓ ~~$L = 2^l - 1$ and l~~ is an integer greater than or equal to the number of bits in M2. (//signifies ~~concentration~~ concatenation).